FORM PTO-1390 (REV. 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 5551

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): 09/937,819

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE00/00189	20 January 2000	29 March 1999

TITLE OF INVENTION: DEVICE AND METHOD FOR SECURE ELECTRONIC DATA TRANSMISSION

APPLICANT(S) FOR DO/EO/US: Volker PAUL; and Bertram BRESSER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☐ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☒ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☐ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)). (verified)
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☒ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). (executed)
10. ☐ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:
    - Verified English translation of International Preliminary Search Report with amended claims 1 and 12;
    - The surcharge of $130 for furnishing the Declaration later than 30 months under 37 CFR 1.492(e) was paid on September 28, 2001.

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/937,819	PCT/DE00/00189	5551

21. ☐ The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1000.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	- 20 =		x $18.00	$	
Independent claims	- 3 =		x $80.00	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $270.00	$	
TOTAL OF ABOVE CALCULATIONS =				$	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.			+	$	
SUBTOTAL =				$	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$ 130.00	
TOTAL NATIONAL FEE =				$ 130.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$ 130.00	
				Amount to be refunded:	$
				charged:	$

10/31/2001 LLANDGRA 00000010 09937819
01 FC:156 130.00 OP

a. ☒ A check in the amount of $ 130.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-3690. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

BREINER & BREINER, L.L.C.
115 North Henry Street
P.O. Box 19290
Alexandria, VA 22320-0290

Date: October 29, 2001

Mary Breiner
SIGNATURE

Mary J. Breiner
NAME

33,161
REGISTRATION NUMBER

5551

CERTIFICATION

I, the undersigned, am a professional translator, fully competent to translate from German into English, and I declare hereby that the attached English rendition of International Application No. PCT/DE00/00189 filed January 20, 2000 entitled

DEVICE AND METHOD FOR SECURE ELECTRONIC DATA TRANSMISSION

is a genuine translation, accurate in every particular, to the best of my ability and knowledge, of the German text, also attached.

Name: Michaela Nierhaus
Address: Brabanterstr. 15
80805 Munich
Germany

Date: Oct. 4, 2001

Device and Method for Secure Electronic Data Transmission

The present invention relates to a device and a method for secure electronic transmission of data between end units that are temporarily or permanently connected to a server.

This method and this device are particlarly suited for electronic transmission of medical data.

From the legal point of view, the confidentiality of medical data has top priority. When transmitting medical data over publicly accessible networks, e.g. the internet or a compound network that is accessible from the outside, it is therefore necessary to provide security measures that ensure the best protection.

The protection mechanisms basically available for data transmission over public networks relate in particular to using cryptographic methods of encoding data. Usually standard cryptographic methods using secure exchange of keys corresponding to X.509 are employed: symmetric encoding processes, in particular for encoding large amounts of data and asymmetrical encoding processes using a so-called public key and a so-called private key, such as the common RSA.

The present invention relates to the transmission of data from one network participant (transmitter) to another (addressee or recipient) via intermediate storage on a data station respectively on a server. Although an asymmetrical encoding process using the public key of the addressee for encoding data offers a high degree of protection in the electronic transmission of data, this method cannot be used by addressees who in many cases are still unknown when the data are provided.
An example of this arises, for instance, in the field of medicine, as explained later on with reference to the preferred embodiment, when a physician gives a patient a transfer slip to

consult a colleague and he wants to send the colleague certain medical data of the patient electronically. In many cases, the identity of the colleague that the patient will seek is not known at the time.

The object of the present invention is to provide a device and a method for secure electronic transmission of data via the server of a network, wherein the addressee of the data does not need to be known at the time when the data is made available.

The object is solved with the device and the method set forth in claims 1 and 12. Advantageous embodiments and further improvements of the device and the method are the subject matter of the subclaims.

The invented device which has to be installed and operated in the network server is provided with an input unit for receiving coded data (from the transmitter) and an external key (of the recipient).
Furthermore, the device has a unit for decoding the coded data with an internal key and for renewed encoding of the data with external key. The internal key is filed in some technical manner inside the device and is not accessible from outside the device. The data encoded with the external key can be retrieved at an output.

It is a matter of course that the to-be processed data have to be encoded in such a manner that they can be decoded with the internal key. Thus, only coded data that the device can read are converted into recoded data inside the device with an external key for recoding. When a corresponding data request is made, the recoded data can be read by the holder of the external key, which was transferred to the device along with the data.

Fundamentally, the original transmitted data, i.e. for example medical data, can be decoded by the device and recoded again.

However, in a preferred application of the device, which is described later on, not the original data itself but only its key transferred in coded form is recoded with the device.

In a preferred embodiment, for decoding the coded data and for recoding the data, the device is provided with a chipcard as carrier of the internal key. This chipcard is preferably a chipcard from a certified trust center.
In another version, encoding and decoding can be partly or completely carried out directly by an active chipcard.

Another possibility is to employ a suited circuit in compliance with information, and communication service and signature laws, if need be software controlled, as a unit for encoding and decoding.

The heart of the invented solution is recoding the data or recoding a key accompanying the data, hereinafter referred to as session key, in such a manner that the data can be read by an authorized communication partner, the addressee. For this purpose, in the preferred embodiment, a session key used for symmetrical encoding of data is decoded with the private key of the server and immediately recoded with the public key of the recipient or addressee requesting the data. This key is preferably stored in the server in a list of participating and authorized network participants, e.g. along with the participant's ID and the ISDN number, and can be updated at any time as needed through the services of a trust center.

Decoding the original data per se is not necessary with this method. Required for later decoding of the data is only the session key, now readable for the recipient, which was generated for instance by chance during encoding as explained in more detail in the preferred embodiment.

In this way, it is avoided that the data are ever in the server uncoded. In detail this means that there is no access to the coded data during the recoding processes at all. Processed is only the session key used for their encoding which was "recoded" in a closed process from a form that only the server respectively the invented device installed in the server can read into a form that the requester can read.

Application of the device is made more apparent by the following preferred embodiment in conjunction with the accompanying figure. This application is in the field of medicine, which is the preferred field of application of the present invention.
In the course of this, security measures which singly are as such already known and which all ensure highly secure data transmission in the mentioned field of application, are explained and executed in combination with the invented device and process.
It is a matter of course, that the combinations of single security measures described in the following are independent of each other so that omitting one of these steps or replacing it by other known security measures is also feasible.

The present example relates to the electronic transmission of medical data over public networks. The security measures used to do this ensure the best possible protection of these sensitive data. In this area, a typical process begins in the office of the doctor of a patient. The physician transfers the patient to a specialized doctor who the physician does not know at this point in time because the patient has the right of free choice.
Hitherto, the patient was usually given a sealed envelope containing the important medical data and the transfer slip which he was to give the specialized doctor of his choice.
If the physician wanted to transmit the data to the colleague electronically, he would have had to know the colleague's identity at the time of the transfer. This is no longer necessary with the process described in the following using the invented device and the invented method. The basic system

comprises at least one central data station, a server, to which a connection can be set up from the data stations participating in the system. In the present case, the data stations are the doctors' external computers. In the described instance, this means the transferring doctor files the patient's required medical data in the server for the (still unknown) colleague and this colleague can retrieve these data from the server at a later date.

The description of the security mechanism starts with the general security aspects of the design of the system and then explains the general and the specific use of the cryptographic process and finally the integration and technical realization of the invented device.

Any form of active reading of data requires, if need be limited, access authority to the data station where the data are stored. In the present example, the system does not permit reading access to the server but only the transmission of a data request through the participating sites. Upon verification of the authority to receive, the data are sent to the requester, in the present case the specialized doctor requesting the data, thereby preventing as far as possible direct access to the data content of the server from an external site.

For communication, the exemplary concept employs a type of communication known as "remote procedure call" (RPC), wherein a request to carry out a certain function and to send back the result of this function is transmitted to the server from an external computer. The advantage of this type of communication is that running on the server is a problem-specific application which executes solely those operations provided in the system function. In this manner, functions that go beyond this, e.g. direct access to the data, are ruled out with absolute certainty.

Furthermore, the concept also provides that in order for a network participant to set up a connection, the network participant first sends a request to set up a connection to the server. This operation itself does not set up a connection. But rather, it is provided that this request is realized as so-called "D channel information". This is a special ISDN network function in which prior to "accepting" a call, thus free of charge, only the identifier respectively the number of the caller is transmitted. Subsequently, the server checks whether the number matches one in the list of participants stored in the server. Only if the transmitted caller's number is one belonging to an "authorized" network participant, will the server initiate a return call via a number stored in an internal data bank.
The special security aspect of this solution is that although the caller's number transmitted in the D channel can, in certain circumstances, be falsified (can be "masked"), the connection via the server is set up in any event with the actual holder of this number, thus the authorized network participant. Therefore, in the worst case, a connection is initiated to a network participant who did not request it but belongs to the authorized group. In any case, no transmission of data occurs, because being unable to provide a data request, the computer of the participant who was called back without requesting the data is unable to set up a connection.

The described exemplary concept is based on transmitting documents once in the sense of "mailing". As soon as a document is requested from the server by an authorized addressee and it is sent to him, it is erased in the server (first logically and then physically). This is particularly possible with the present application, because the data are only intended for one addressee.
If the data are to be accessible to several addressees, this measure is not provided.
Moreover, all the data are provided with an expiration date. When it has expired, the data are also erased physically. In this

manner, data do not accumulate in the server, thus making it impossible to link different documents relating to one patient or to one doctor. The identification of the documents occurs via a procedure ID granted only once for this specific communication procedure and does not permit drawing any conclusions about the patient. The requesting doctor must know this ID, and it is preferably given to him with the respective paper document (transfer slip) by the patient himself.

In addition to the described security measures, all the data are encoded and signed for the transmission and storage utilizing standard cryptographic processes with a secure exchange of keys, for example corresponding to X.509. These are symmetric encoding processes such as triple DES, "blowfish" or IDEA for encoding large amounts of data and asymmetrical encoding processes such as RSA or elliptical encoding processes for the digital signature (encoding a hash value) and the encoding of the symmetrical session key.

In order to secure the authenticity and the integrity of the transmitted data, each document is signed before transmission with the sender's private key, in the present case the transferring doctor's. For this purpose a hash value is determined which is asymmetrically encoded with the sender's private key. The signature of the document is preserved even after decoding (see following steps) and thus is at disposal for forensic relevant verification of the authenticity of the document. However, a prerequisite for the proof of authenticity is that the document is stored in the signed form at the recipient, if need be also an unsigned version is stored there in addition to the readable one. Separate storage of the document and the signature is possible. However, it has the danger that unintended modification of the document, e.g. when opening the word processing system, invalidates the signature. Archiving the document is the recipient's responsibility.

The single documents are symmetrically encoded using a random generating key (session key) with a length of N (for security reasons N should be larger than or equal 128). The session key employed for encoding is encoded with the server's public key, i.e. the invented device installed in the server. For security reasons, the length of the key should be at least 1024 bits.

As the document including the signature are encoded, the server cannot check the authenticity of a document, neither with regard to its error-free transmission nor its existence per se (electronic "registration"), without decoding the data. In order to permit this, the signed and encoded document is signed again in addition.

The document prepared in the aforedescribed manner is processed as a MIME-compatible file and transmitted in this form to the server by means of a corresponding RPC. In the server, the document is unpacked out of the MIME format and the external signature is checked and removed in the process. In this manner, its intactness, i.e. the completeness and authenticity of the document, is checked and then logged. After successful filing of the (encoded) document, a receipt signed with the server's personal key is returned to the sender by the server as infallible proof of successful filing of the document.

The to-be-forwarded document is stored in the server in the (internally) signed and then encoded form. No one can decode it in this coded form.
An accompanying not coded procedure ID, which is part of each procedure, serves as filing respectively access criterium for administering the coded documents. As already explained in the preceding, this procedure ID is given later by the patient directly to the doctor of his choice. This ID is clear to the server from the transmitted request for data of which it is a part.

Data can be requested by participants of the respective network by providing this respective procedure ID, their ISDN number and their doctors's identifier.
Additional identifiers, e.g. for distinguishing the respective patient, may be required to increase security further.

When the respective specialist doctor requests data, the invented device recodes the data in such a manner that it becomes readable for the requesting doctor. For this purpose, the session key employed for symmetrically encoding the data is decoded with the server's private key present in the server and immediately recoded with the requesting recipient's public key. This public key is, along with the doctor's ID and the ISDN number, stored in the list of participating network doctors and can be updated via the service of a participating trust center.
It is not necessary to decode the medical data itself. In order to later decode the data, only the session key, now readable for the recipient, has to be known which was randomly generated in the course of encoding.
In this manner, it is impossible that the medical data themselves are present in the server in an uncoded form at any time. There is no access to the coded data during recoding. Processed is solely the session key used for their encoding and which is "recoded" from a form only readable for the server into a form readable for the requester.

The document encoded for transmission to the recipient is signed again to secure correct transmission to the recipient and to secure possibly desired logging, notably by the server with its personal key.

The document prepared in the manner described in the preceding is processed as a MIME compatible file and is sent in this form as a RPC reply to the data request to the requester.

At the recipient the document is unpacked out of the MIME format, the external signature is checked and in the process removed. In this manner, the intactness, i.e. the completeness and the authenticity, of the document is checked again. The recipient's receipt signed with his personal key is returned to the server as infallible proof of successful transmission of the document.

The recipient can decode the coded session key with his personal key and then decode the data themselves with it. Following this, the data are present only in the form that is readable with the sender's signature.

The purpose of the signature of the initial document is to be able to prove the docucent's authenticity. In order to preserve the signature, it is necessary to store the document in the signed form.

A possible vulnerable point is the server's private key. As all the stored data, more precisely all the session keys of the stored data, can be read with the same server's key, it would pay, in particular, to attack this key and, on the other hand, an attack is facilitated by the amount of data present.
In order to take precautions against this circumstance, in a preferred embodiment of the present invention, as an additional security mechanism, it is provided that the session key is split in two.

As described in the preceding, the original data is encoded with a N-bit (N being preferably greater than or equaling 128 bits) symmetrical key. This key is usually asymmetrical for transmission and only encoded in a manner that is readable to the recipient. Decoding, even forcible decoding, the session key thus suffices to be able to decode the data itself.

In order to prevent this, the following modification is introduced. In this modification, the session key is split in two before its symmetrical encoding. For instance, M ($0 < M < N$) of the N bits of the session key are removed as a so-called "procedure key". Only the remaining (N-M) bits of the session keys are asymmetrically encoded and transmitted along with the data.
Recoding the data with the reduced session key occurs in the same manner as described in the preceding in connection with a whole session key. As the data themselves never have to be decoded there, the whole session key is not required. Only the rudimentary session key is decoded by the server and encoded again for the requester.

Decoding at the recipient differs from the aforedescribed procedure in that after decoding of the session key by means of the recipient's private key, this session key has to be expanded by the M bits of the procedure key separated at the sender. Following this, decoding can occur as described in the preceding.

The procedure key generated at the sender of the data, i.e. the separated M bits, are added to the procedure ID which was also generated there. A combination of the procedure ID and the procedure key yields the so-called procedure identifier which is printed on the accompanying paper document (transfer slip, prescription, ...) and read at the recipient. The procedure key contained in the procedure identifier is never transmitted to the server so that all the information required to actually decode a document never comes together in the server.

Figure 1 shows an example of the invented device as utilized for carrying out the preceding application example.
The device is preferably designed in the form of a plug-in module 1 (recoding module) for modular installation in the server. In the present case, module 1 contains a chipcard 2 which conducts the decoding of the coded session key 10a with the aid of the

server's private key stored in the chipcard 2 and the recoding of the session key with the public key of the addressees respectively the requesters of the data. The server's private key is not accessible from outside the chipcard respectively from outside the module. The requester's public key is conveyed to device 1, as is the to-be-recoded session key 10a, via an interface provided for this purpose. The recoded session key 10b is issued via a further interface.

The server's processor itself assumes the task of separating the session key 10a from the coded data block 11, conveying it to device 1 and adding the session key 10b supplied and recoded by the device to data block 11 again, as the diagram in the figure shows.

However, this separation and renewed combination can also be conducted directly in device 1. In this case, the entire data block 11 with the session key 10a would have to be conveyed to the device.

The server's personal key is undoubtedly a critical point with regard to intentional, unauthorized attempts to gain access to the data.

Usually keys must not respectively should not be stored in the computer on which the coded data are stored respectively are processed. However, if the server operates automatically as in the present case this is unavoidable. For this reason, in the present embodiment the device is designed as a sealed, encapsulated unit that is able to carry out the entire procedure of recoding the data internally without the decoded (even rudimentary) session key or even only traces of its decoding leaving the autonomous unit.

Today there are already key cards available on the market that are able to carry out the asymmetrical encoding of a 128-bit session key according to a 1024-bit RSA process completely on the chip of the card. Soon such cards will also be available for 2048-bit keys.

In particular, there is the possibility to have the two keys (public key - private key) generated directly on the card or in a lawful, certified trust center without the private key of the card ever leaving the card. Such a key card can be utilized in the invented device as chipcard 2. In a first step, the coded session key 10a is conveyed to this chipcard 2. This coded session key 10a is then decoded with the aid of the card's private key, which in the preceding was referred to as the server's private key. The decoded session key is issued by card 2 without, however, ever leaving device 1. But rather in a second step of card 2, it is entered again, this time along with the addressee's public key. In this second step, card 2 returns the recoded session key 10b. This is shown by arrows inside device 1 in the figure. The additional circuit, buffer unit 4, required for this serves, i.a. to coordinate these procedures temporally. This buffer unit 4 can, for example, be realized by a suited, programmed micro the coded session key 10a processor or by means of a logic circuit.

In order to prevent drawing conclusions about the internal procedures from the modulations on the current supply of the device, in the present embodiment of the device, a constant current circuit 3 is provided which ensures within the scope of a defined interval of the supply voltage that the device is provided with a constant and modulation-free current input. When exceeding or falling short of certain limits of the operating voltage or other operation parameters, such as, e.g. temperature, the device turns off with an error message.

As conclusions can also be drawn about the internal procedures from the temporal behavior of the device, all the input data can be first buffered in the buffer unit 4 or in a special unit provided for this purpose and the results can be issued after always the same time regardless of how much time the internal procedures took.

"Bugging" the electronic procedures in the device is prevented in the present embodiment by an electromagnetic screening 5 of the device.

Provided as the interface of the device is, on the one hand, an interface for the input of the asymmetrically encoded session key 10a (respectively a rudiment of this key) and of the public key of the requesting recipient. On the other hand, an interface must be provided for the output of the asymmetrically encoded session key 10b (respectively its rudiment). Both interfaces can be physically identical with a suited design.
Furthermore, for generating respectively checking signatures, interfaces can be provided for the input of the hash value of the to-be signed document and for the output of the symmetrically encoded hash value, i.e. the signature.

Although the aforedescribed measures were presented in the context of the example on which the present invention is based, this idea and the invented device can, of course, also be applied in other fields requiring secure transmission of data between two data stations via intermediate storage on a server.

Furthermore, the present invention is not limited to the transmission of data only via one intermediate station respectively one server. The data can also be transmitted via multiple servers, with the data request being executed by another server always in the same manner as the request by an addressee. Then the data are treated in the other server in the same manner as in the first server, i.e. this other server must also be provided with the invented device.

What is Claimed Is:

1. A device for secure transmission respectively forwarding of coded data via a data station of a network, having
- an input unit for receiving said coded data (10a) and an external key;
- a unit (2) for decoding said coded data with an internal key and recoding said data with said external key, with said internal key not being accessible from outside said device; and
- an output unit for issuing said data (10b) encoded with said external key.

2. A device according to claim 1,
wherein said internal key is stored on a suited data carrier inside said unit (2) for decoding and encoding.

3. A device according to claim 1 or 2,
wherein said unit (2) for decoding and encoding comprises a chip card as said carrier of said internal key.

4. A device according to claim 1 or 2,
wherein said unit (2) for decoding and encoding comprises an active chip card with an integrated processor, which partly or completely assumes the decoding and encoding of said data.

5. A device according to one of the claims 1 to 4,
wherein said device is provided with a buffer and logic unit (4) for temporal control of the data flow in said device, said buffer and logic unit (4) first conveys said coded data (10a) for decoding to said unit (2) for decoding and encoding and receives said data back decoded, and said buffer and logic unit (4) subsequently conveys said decoded data for encoding with said external key to said unit (2) for decoding and encoding and receives it back as coded data (10b).

6. A device according to one of the claims 1 to 5, wherein said input unit and said output unit are provided with standard interfaces for the input and output of said data.

7. A device according to one of the claims 1 to 6, wherein said unit (2) for encoding and decoding utilizes asymmetrical encoding processes.

8. A device according to one of the claims 1 to 7, wherein said device is provided with a complete mechanical and electromagnetic encapsulation (5) and with a possibility of sealing.

9. A device according to one of the claims 1 to 8, wherein a buffer unit is provided which buffers all the data flows inside said device to compensate for possible internal-key-dependent processing times so that the data output of said device occurs according to a process-independent time span.

10. A device according to one of the claims 1 to 9, wherein a unit (3) is provided for buffering the current input of said device in such a manner that said current input of said device is independent of the current input of said unit (2) for decoding and encoding, which is dependent on said internal key, or of other internal circuits.

11. A device according to one of the claims 1 to 10, which is further provided with a unit for receiving a first data block containing said coded data (10a) in addition to further data (11) and for separating said coded data (10a) from said further data (11) and with a unit for joining said further data (11) with the recoded data (10b) to a second data block and for the output of said second data block, with said encoded data representing a key with which said further data (11) are encoded.

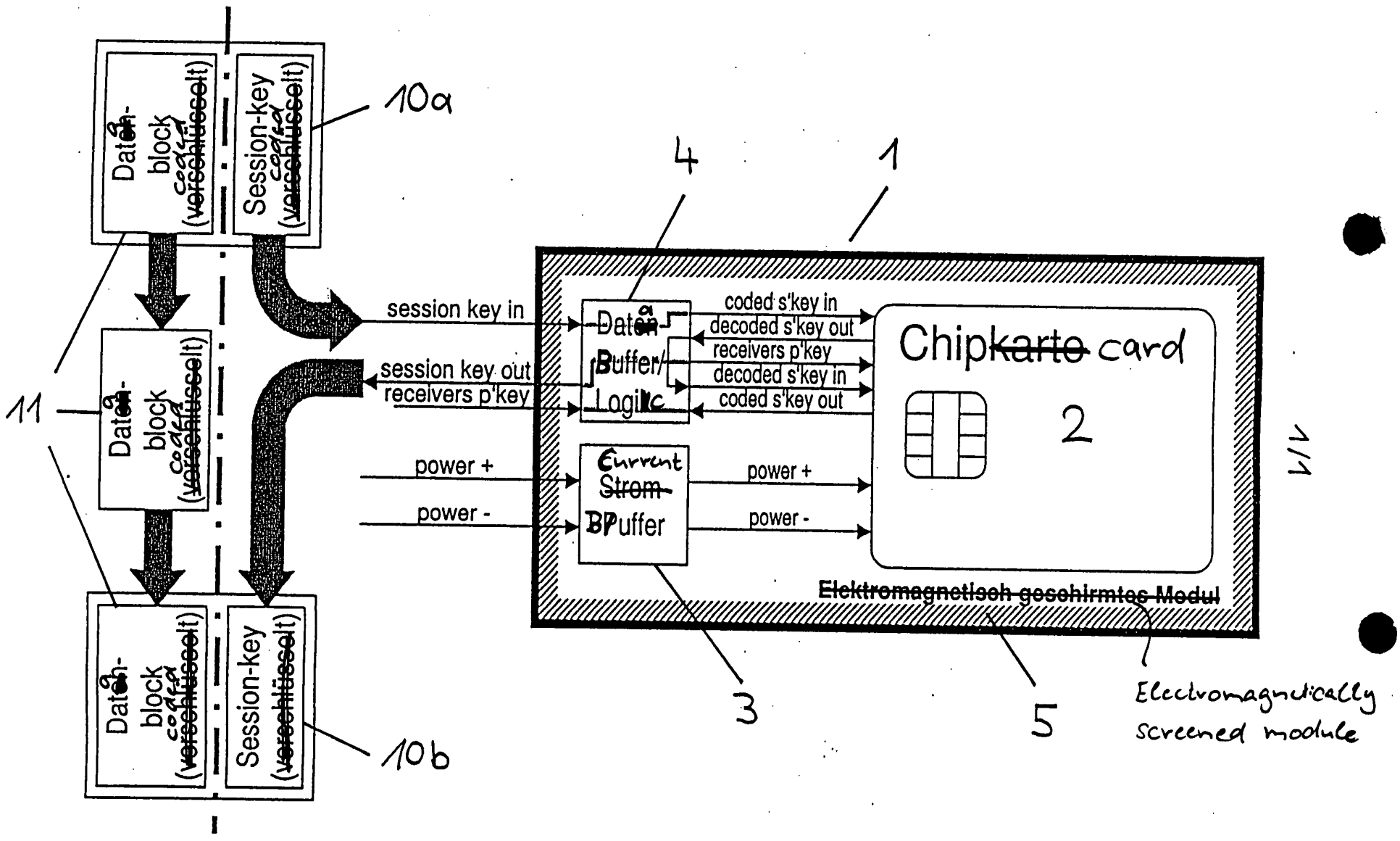
12. A process for secure data transmission from a first data station via a second data station to a third data station using the device according to one of the preceding claims, having the following steps:
- encoding of the data in said first data station with a first key;
- encoding of at least a part of said first key in said first data station with a public key of said second data station;
- transmission of said coded data (11) together with the coded part of said first key (10a) to said second data station;
- storage of said coded data (11) and of said coded part of said first key (10a) in said second data station;
- request of said data by said third data station;
- decoding of said coded part of said first key with a private key of said second data station matching said public key and recoding of the previously decoded part of said first key with a public key of said third data station; and
- transmission of said coded data (11) together with said recoded part of said first key (10b) to said third data station.

13. A process according to claim 12, whereby said first key is completely encoded and transmitted.

14. A process according to claim 12, whereby only a part of said first key is encoded and transmitted to said second data station.

15. A process according to one of the claims 12 to 14, whereby said coded part of said first key is decoded in said third data station with said private key of said third station and subsequently said data (11) are decoded with said first key.

16. A process according to one of the claims 12 to 15, whereby said public key of said third data station is taken from an internal data bank of said second data station or is determined by consultation with a trust center.


Daten-block coded (verschlüsselt)
Session-key coded (verschlüsselt)
10a
11
Daten-block coded (verschlüsselt)
Daten-block coded (verschlüsselt)
Session-key (verschlüsselt)
10b
session key in
session key out
receivers p'key
power +
power -
4
1
Daten-Buffer/ Logic
Current Strom BPuffer
coded s'key in
decoded s'key out
receivers p'key
decoded s'key in
coded s'key out
power +
power -
Chipkarte card
2
Elektromagnetisch geschirmtes Modul
3
5
Electromagnetically screened module
1/1

Vorrichtung und Verfahren für die sichere elektronische Datenübertragung

Die Erfindung betrifft eine Vorrichtung sowie ein Verfahren für die sichere elektronische Datenübertragung zwischen Endgeräten, die zeitweilig oder permanent mit einem Server verbunden sind.

Das Verfahren und die Vorrichtung sind insbesondere für die elektronische Weitergabe medizinischer Daten sehr gut geeignet.

Medizinische Daten stellen aus der rechtlichen Sicht des Datenschutzes eines der schützenswertesten Güter überhaupt dar. Für die elektronische Weitergabe medizinischer Daten über öffentlich zugängliche Netze, wie beispielsweise das Internet oder ein von außen zugängliches Verbundnetz, sind daher Sicherheitsmaßnahmen vorzusehen, die den bestmöglichen Schutz solcher Daten gewährleisten.

Die grundsätzlich für die Datenübertragung durch öffentliche Netze verfügbaren Sicherheitsmechanismen betreffen vor allem die Nutzung kryptographischer Verfahren zur Verschlüsselung der Daten. Hierbei werden in der Regel kryptographische Standardverfahren mit sicherem Austausch von Schlüsseln entsprechend X.509 eingesetzt. Dabei handelt es sich um symmetrische Verschlüsselungsverfahren, insbesondere für die Verschlüsselung großer Datenmengen, und um asymmetrische Verschlüsselungsverfahren unter Verwendung eines öffentlichen (sog. "public key") und eines

privaten Schlüssels (sog. "private key"), wie das weit verbreitete RSA.

Die vorliegende Erfindung betrifft die Übertragung von Daten von einem Netzteilnehmer (Absender) zu einem anderen (Adressat bzw. Empfänger) über die Zwischenspeicherung auf einer Datenstation bzw. einem Server. Während bei der elektronischen Datenübertragung über das Netz von einem Teilnehmer zu einem bereits bekannten Adressaten ein asymmetrisches Verschlüsselungsverfahren unter Verwendung des öffentlichen Schlüssels des Adressaten zur Verschlüsselung der Daten eine hohe Datensicherheit bietet, kann diese Vorgehensweise bei einem zum Zeitpunkt der Bereitstellung der Daten noch unbekannten Adressaten nicht eingesetzt werden.

Ein solcher Fall ergibt sich beispielsweise im medizinischen Bereich, wie weiter unten im Ausführungsbeispiel näher erläutert wird, wenn ein Arzt einem Patienten eine Überweisung an einen Kollegen ausstellt und die für den Arztkollegen bestimmten medizinischen Daten des Patienten auf elektronischem Wege bereitstellen will. Die Identität des Kollegen, den der Patient schließlich aufsuchen wird, ist zu diesem Zeitpunkt in vielen Fällen noch nicht bekannt.

Die Aufgabe der vorliegenden Erfindung besteht nun darin, eine Vorrichtung und ein Verfahren für die sichere elektronische Datenübertragung über den Server eines Netzwerkes bereitzustellen, bei dem der Adressat der Daten zum Zeitpunkt der Bereitstellung der Daten noch nicht bekannt sein muß.

Die Aufgabe wird mit der Vorrichtung und dem Verfahren nach den Ansprüchen 1 und 12 gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen des Verfahrens und der Vorrichtung sind Gegenstand der Unteransprüche.

Die erfindungsgemäße Vorrichtung, die am Server des Netzwerkes installiert und betrieben werden muß, weist eine Eingangseinheit zum Empfangen von verschlüsselten Daten (des Absenders) sowie eines externen Schlüssels (des Empfängers) auf. Weiterhin ist in der Vorrichtung eine Einheit zum Entschlüsseln der verschlüsselten Daten mit einem internen Schlüssel und zum erneuten Verschlüsseln der Daten mit dem externen Schlüssel vorgesehen. Der interne Schlüssel ist innerhalb der Vorrichtung in irgendeiner technischen Form abgelegt und von außerhalb der Vorrichtung nicht zugänglich. An einer Ausgangseinheit können die mit dem externen Schlüssel verschlüsselten Daten abgegriffen werden.

Es versteht sich von selbst, daß die von der Vorrichtung zu verarbeitenden Daten so verschlüsselt sein müssen, daß sie mit dem internen Schlüssel der Vorrichtung entschlüsselt werden können. In der Vorrichtung werden somit nur für die Vorrichtung lesbare verschlüsselte Daten mit einem externen Schlüssel zur Neuverschlüsselung umgewandelt in neu verschlüsselte Daten, die für den Inhaber des bei einer entsprechenden Datenanforderung mit den Daten an die Vorrichtung übergebenen externen Schlüssels lesbar sind.

Hierbei ist es grundsätzlich möglich, die zu übertragenden Ursprungsdaten, d.h. beispielsweise medizinische Daten, von der Vorrichtung entschlüsseln sowie neu verschlüsseln zu lassen. Bei dem bevorzugten Einsatz der Vorrichtung, wie weiter unten ausgeführt, werden allerdings nicht die Ursprungsdaten selbst, sondern nur deren in verschlüsselter Form übertragener Schlüssel mit der Vorrichtung neu verschlüsselt.

In einer bevorzugten Ausführungsform weist die Vorrichtung zum Entschlüsseln der verschlüsselten Daten sowie zur Neuverschlüsselung der Daten eine Chipkarte als Träger des internen Schlüssels auf. Bei dieser Chipkarte handelt es sich vorzugsweise um eine Chipkarte eines zertifizierten Trust-Centers.

In einer weiteren Ausprägung können Verschlüsselung und Entschlüsselung ganz oder teilweise direkt durch eine aktive Chipkarte ausgeführt werden.

Eine weitere Möglichkeit besteht darin, eine nach dem Informations- und Kommunikationsdienste-Gesetz sowie Signaturgesetz geeignete Schaltung, gegebenenfalls Software-gesteuert als Einheit zur Ver- und Entschlüsselung einzusetzen.

Kern der erfindungsgemäßen Lösung ist eine Umschlüsselung der Daten oder eines den Daten anhängenden Schlüssels, im folgenden als Session-Key bezeichnet, so daß die Daten für einen der berechtigten Kommunikationspartner, den Adressaten, lesbar werden. Dazu wird in der bevorzugten Ausführungsform des Verfahrens ein für die symmetrische Verschlüsselung der Daten verwendeter Session-Key mit dem im Server vorhandenen priva-

ten Schlüssel des Servers entschlüsselt und sofort wieder mit dem öffentlichen Schlüssel des die Daten anfordernden Empfängers bzw. Adressaten verschlüsselt. Dieser Schlüssel ist vorzugsweise - z.B. zusammen mit der Teilnehmer-ID und der ISDN-Nummer - in einem Verzeichnis der beteiligten und berechtigten Netzteilnehmer auf dem Server gespeichert und kann bei Bedarf über die Dienste eines Trust-Centers jederzeit aktualisiert werden.

Ein Entschlüsseln der Ursprungsdaten selbst ist bei diesem Verfahren nicht notwendig. Zum späteren Entschlüsseln der Daten muß nur der - jetzt für den Empfänger lesbare - Session-Key bekannt sein, der bei der Verschlüsselung beispielsweise per Zufall generiert wurde, wie im Ausführungsbeispiel näher erläutert wird.

Auf diese Weise wird vermieden, daß die Daten selbst zu irgendeinem Zeitpunkt auf dem Server in unverschlüsselter Form vorliegen. Im Detail bedeutet dies, daß auf die verschlüsselten Daten während des Umschlüsselungsprozesses überhaupt kein Zugriff erfolgt. Verarbeitet wird lediglich der für Ihre Verschlüsselung verwendete Session-Key, der in einem geschlossenen Prozeß aus einer nur für den Server bzw. die am Server installierte erfindungsgemäße Vorrichtung lesbaren in eine für den Anfordernden lesbare Form "umgeschlüsselt" wird.

Der Einsatz der Vorrichtung soll im nachfolgenden anhand eines Ausführungsbeispiels in Verbindung mit der Figur näher erläutert werden. Dieses Beispiel betrifft einen Anwendungsfall im medizinischen Bereich, der ein

bevorzugtes Anwendungsfeld der vorliegenden Erfindung darstellt.

Hierbei werden in Kombination mit der erfindungsgemäßen Vorrichtung sowie dem erfindungsgemäßen Verfahren weitere, für sich genommen bereits bekannte Sicherheitsmaßnahmen beschrieben und vorgenommen, die insgesamt eine hochsichere Datenweitergabe in dem genannten Anwendungsfall gewährleisten.

Es versteht sich von selbst, daß die nachfolgend angeführten Kombinationen der einzelnen Sicherheitsmaßnahmen unabhängig voneinander sind, so daß auch die Auslassung eines dieser Schritte, oder der Ersatz durch andere bekannte Sicherheitsmaßnahmen, möglich sind.

Das Beispiel betrifft die elektronische Weitergabe medizinischer Daten über öffentliche Netze. Die hierfür eingesetzten Sicherheitsmaßnahmen gewährleisten den bestmöglichen Schutz dieser sensiblen Daten. Ein typischer Vorgang in diesem Bereich beginnt in der Praxis des Arztes eines Patienten. Der Arzt überweist den Patienten an einen Facharzt, der diesem aufgrund des freien Arztwahlrechtes des Patienten zu diesem Zeitpunkt noch nicht bekannt ist. Üblicherweise wurden dem Patienten bisher hierzu in einem verschlossenen Umschlag die für den Facharzt wichtigen medizinischen Daten zusammen mit der Überweisung übergeben, der diese dem von ihm gewählten Facharzt dann weitergegeben hat.

Wollte der Arzt diese Daten dem Kollegen auf elektronischem Wege übermitteln, so mußte er bisher die Identität dieses Kollegen zum Zeitpunkt der Überweisung bereits kennen. Dies ist mit dem im folgenden geschilderten Verfahren unter Einsatz der erfindungsgemäßen Vorrichtung und des erfindungsgemäßen Verfahrens nicht

mehr erforderlich. Das zugrunde liegende System sieht zumindest eine zentrale Datenstation, einen Server, vor, zu dem von Datenstationen der am System beteiligten Stellen, im vorliegenden Fall den externen Rechnern der Ärzte, eine Verbindung hergestellt werden kann. Bezogen auf den oben dargestellten Fall bedeutet dies, daß der überweisende Arzt die für den (noch unbekannten) Kollegen vorgesehenen medizinischen Daten des Patienten auf dem Server ablegt, von dem sich der Kollege diese Daten dann zu einem späteren Zeitpunkt holen kann.

Die Beschreibung der Sicherheitsmechanismen geht dabei zunächst von allgemeinen Sicherheitsaspekten des Systemdesigns aus, beschreibt dann die allgemeine und spezielle Nutzung kryptographischer Verfahren und schließlich die Einbindung und technische Umsetzung der erfindungsgemäßen Vorrichtung.

Jede Form des aktiven Lesens von Daten erfordert ein - gegebenenfalls eingeschränktes - Zugriffsrecht auf die Datenstation, auf der die Daten gespeichert sind. Im vorliegenden Beispiel gestattet das System keinen lesenden Zugriff auf den Server, sondern nur das Absetzen einer Datenanforderung durch die beteiligten Stellen. Bei nachgewiesener Empfangsberechtigung werden die Daten dem Anforderer, im vorliegenden Beispiel also dem die Daten anfordernden Facharzt, über das Netz zugeschickt. Dadurch werden direkte Zugriffe einer externen Stelle auf Datenbestände des Servers weitestgehend unterbunden.

Das beispielhafte Konzept verwendet für die Kommunikation eine Kommunikationsart, die als "remote procedure call" (RPC) bekannt ist. Dabei wird vom externen Rechner eine Aufforderung an den Server gesendet, eine bestimmte Funktion auszuführen und das Ergebnis dieser Funktion als Resultat zurückzugeben. Der Vorteil dieser Kommunikation ist, daß auf dem Server eine problemspezifische Applikation läuft, die nur genau die Operationen ausführt, die in der Systemfunktion vorgesehen sind. Darüber hinausgehende Funktionen, wie z.B. ein direkter Dateizugriff, sind auf diese Weise absolut sicher ausgeschlossen.

Das Konzept sieht weiterhin vor, daß ein Netzteilnehmer zum Aufbau einer Verbindung zunächst immer eine Aufforderung zum Verbindungsaufbau an den Server schickt. Bei dieser Operation selbst erfolgt noch kein Verbindungsaufbau. Es ist vielmehr vorgesehen, diese Anforderung als sogenannte "D-Kanal-Nachricht" zu realisieren. Dabei handelt es sich um eine spezielle Funktion des ISDN-Netzes, bei der noch vor dem "Annehmen" eines Gespräches - damit auch gebührenfrei - nur die Kennung bzw. Nummer des Anrufers übermittelt wird. Anschließend prüft der Server die Übereinstimmung dieser Nummer mit einer am Server gespeicherten Teilnehmerliste, und nur wenn die übermittelte Nummer des Anrufers zu einem "berechtigten" Netzteilnehmer gehört, initiiert der Server einen Rückruf über eine in einer internen Datenbank gespeicherte Nummer.

Der besondere Sicherheitsaspekt dieser Lösung besteht darin, daß zwar die im D-Kanal übertragene Nummer des Anrufers unter bestimmten Umständen

fälschbar ("maskierbar") ist, die Verbindung durch den Server aber in jedem Fall mit dem tatsächlichen Inhaber dieser Nummer, also einen berechtigten Netzteilnehmer aufgebaut wird. Damit wird im ungünstigsten Falle ein Verbindungsaufbau zu einem Netzteilnehmer angestoßen, der diesen gar nicht angefordert hatte, jedoch zum Kreis der Berechtigten gehört. In einem derartigen Fall kann es zu keiner Datenübertragung kommen, da der Rechner des unaufgefordert zurückgerufenen Teilnehmers keine Datenanforderung bereithält, und damit auch nicht zum Verbindungsaufbau bereit ist.

Das vorliegend beschriebene beispielhafte Konzept basiert darauf, Dokumente im Sinne eines "Mailings" einmalig zu übertragen. Sobald ein Dokument vom Server durch einen berechtigten Adressaten abgefordert und diesem zugestellt wurde, wird es auf dem Server gelöscht (zunächst logisch, dann auch physisch). Dies ist speziell im vorliegenden Anwendungsfall möglich, da die Daten jeweils nur für einen Adressaten vorgesehen sind. Sollen die Daten mehreren Adressaten zugänglich sein, wird diese Maßnahme nicht vorgesehen.

Alle Dokumente werden weiterhin mit einem Verfallsdatum versehen, nach dessen Ablauf sie ebenfalls physisch gelöscht werden. Damit entsteht keine Akkumulation von Daten auf dem Server, womit auch die Zusammenführung von unterschiedlichen Dokumenten, die etwas über einen Patienten oder auch über einen Arzt aussagen könnten, unmöglich gemacht wird. Die Identifikation der Dokumente erfolgt über eine einmalig nur für diesen Kommunikationsvorgang vergebene Vorgangs-ID, die keinen Rückschluß auf den Patienten zuläßt. Diese ID muß dem anfordernden Arzt bekannt sein, und wird ihm

vorzugsweise mit dem zugehörigen Papierdokument durch den Patienten übermittelt.

Zusätzlich zu den oben beschriebenen Sicherheitsmaßnahmen werden alle Daten für die Übertragung und Speicherung verschlüsselt und signiert. Dazu werden kryptographische Standardverfahren mit sicherem Austausch von Schlüsseln, beispielsweise entsprechend X.509, eingesetzt. Dabei handelt es sich um symmetrische Verschlüsselungsverfahren wie Triple DES, "blowfish" oder IDEA für die Verschlüsselung großer Datenmengen und asymmetrische Verschlüsselungsverfahren wie RSA oder elliptische Verschlüsselungsverfahren für die digitale Signatur (Verschlüsselung eines Hash-Wertes) und die Verschlüsselung des symmetrischen Session-Keys.

Zur Sicherung der Authentizität und Integrität der übertragenen Daten wird jedes Dokument vor dem Versand mit dem privaten Schlüssel des Absenders, im vorliegenden Fall des überweisenden Arztes, signiert. Dazu wird ein Hash-Wert ermittelt und dieser mit dem privaten Schlüssel des Absenders asymmetrisch verschlüsselt. Die Signatur des Dokumentes bleibt auch nach dem Entschlüsseln (siehe nachfolgende Schritte) erhalten und steht somit für den forensisch relevanten Nachweis der Echtheit des Dokumentes zur Verfügung. Voraussetzung für den Nachweis der Echtheit ist allerdings, daß das Dokument beim Empfänger in der signierten Form gespeichert wird, gegebenenfalls zusätzlich zur lesbaren Version ohne Signatur. Ein getrenntes Speichern von Dokument und Signatur ist möglich, birgt jedoch die Gefahr, daß durch ungewollte Modifikation des Dokumen-

tes - z.B. beim Öffnen im Textverarbeitungssystem - die Signatur ungültig wird. Die Archivierung des Dokuments obliegt dem Empfänger.

Die Einzeldokumente werden mit einem zufällig generierten Schlüssel (Session-Key) der Länge N (N sollte aus Sicherheitsgründen größer oder gleich 128 sein) symmetrisch verschlüsselt. Der zum Verschlüsseln verwendete Session-Key wird mit dem öffentlichen Schlüssel des Servers, d.h. der am Server installierten erfindungsgemäßen Vorrichtung, verschlüsselt. Die Schlüssellänge sollte aus Sicherheitsgründen mindestens 1024 Bit betragen.

Da das Dokument inklusive Signatur verschlüsselt wird, kann der Server ohne Entschlüsselung der Daten die Echtheit des Dokumentes - auch im Sinne seiner fehlerfreien Übertragung und seiner Existenz an sich (elektronisches "Einschreiben") - nicht überprüfen. Um dies zu ermöglichen, wird das signierte und verschlüsselte Dokument nochmals zusätzlich signiert.

Das wie oben beschrieben vorbereitete Dokument wird als MIME-kompatibles File aufbereitet und in dieser Form mittels eines entsprechenden RPC an den Server übermittelt.

Auf dem Server wird das Dokument aus dem MIME-Format entpackt und die äußere Signatur kontrolliert und dabei entfernt. Damit wird die Unversehrtheit, d.h. die Vollständigkeit und Originalität, des Dokumentes überprüft und kann protokolliert werden. Nach erfolgter Ablage des (verschlüsselten) Dokumentes wird eine vom

Server mit dessen persönlichem Schlüssel signierte Empfangsbestätigung an den Absender zurückgegeben als zweifelsfreier Nachweis der erfolgten Ablage des Dokumentes.

Das weiterzuleitende Dokument wird auf dem Server in der (innen) signierten und dann verschlüsselten Form gespeichert. In dieser verschlüsselten Form ist es von niemandem zu entschlüsseln.

Als Ablage- bzw. Zugriffskriterium zum Verwalten des verschlüsselten Dokuments dient eine unverschlüsselt mitgelieferte Vorgangs-ID, die zu jedem Vorgang gehört. Diese Vorgangs-ID, wird, wie bereits oben dargelegt, dem später durch den Patienten ausgewählten Arzt durch diesen auf direktem Wege übermittelt. Für den Server ist diese ID aus der übersandten Datenanforderung ersichtlich, deren Bestandteil sie ist.

Daten können vom Server durch Mitglieder des jeweiligen Netzes unter Angabe dieser jeweiligen Vorgangs-ID, ihrer ISDN-Nummer und ihrer Arztkennung angefordert werden.

Zur weiteren Erhöhung der Sicherheit können zusätzliche Identifikatoren, z.B zur Kennzeichnung des jeweiligen Patienten, notwendig sein.

Bei der Anforderung der Daten durch den betreffenden Facharzt erfolgt eine Umschlüsselung der Daten durch die erfindungsgemäße Vorrichtung, so daß sie für einen den anfordernden Arzt lesbar werden. Dazu wird der für die symmetrische Verschlüsselung der Daten verwendete Session-Key mit dem im Server vorhandenen privaten Schlüssel des Servers entschlüsselt und sofort

wieder mit dem öffentlichen Schlüssel des anfordernden Empfängers verschlüsselt. Dieser öffentliche Schlüssel ist - zusammen mit der Arzt-ID und der ISDN-Nummer - im Verzeichnis der beteiligten Netzärzte gespeichert und kann über die Dienste eines einbezogenen Trust-Centers jederzeit aktualisiert werden.

Ein Entschlüsseln der medizinischen Daten selbst ist nicht notwendig. Zum späteren Entschlüsseln der Daten muß nur der - jetzt für den Empfänger lesbare - Session-Key bekannt sein, der bei der Verschlüsselung per Zufall generiert wurde.

Auf diese Weise wird vermieden, daß die medizinischen Daten selbst zu irgendeinem Zeitpunkt auf dem Server in unverschlüsselter Form vorliegen. Auf die verschlüsselten Daten erfolgt während des Umschlüsselungsprozesses keinerlei Zugriff. Verarbeitet wird lediglich der für Ihre Verschlüsselung verwendete Session-Key, der in einem geschlossenen Prozeß aus einer nur für den Server lesbaren in eine für den Anfordernden lesbare Form "umgeschlüsselt" wird.

Das für den Versand an den Empfänger verschlüsselte Dokument wird nochmals zur Sicherung der korrekten Übertragung zum Empfänger und einer eventuell gewünschten Protokollierung signiert, und zwar durch den Server mit dessen persönlichem Schlüssel.

Das wie oben beschrieben vorbereitete Dokument wird wiederum als MIME-kompatibles File aufbereitet und in dieser Form als Rückgabewert eines RPC zur Datenanforderung an den Anforderer geschickt.

Beim Empfänger wird das Dokument aus dem MIME-Format entpackt und die äußere Signatur kontrolliert und dabei entfernt. Damit wird wiederum die Unversehrtheit, d.h. Vollständigkeit und Originalität, des Dokumentes überprüft. Eine vom Empfänger mit dessen persönlichem Schlüssel signierte Empfangsbestätigung wird an den Server zurückgegeben als zweifelsfreier Nachweis der erfolgten Übermittlung des Dokumentes.

Mittels des persönlichen Schlüssels des Empfängers kann dieser den verschlüsselten Session-Key entschlüsseln und mit diesem wiederum die Daten selbst. Danach liegen diese lesbar nur noch in der durch den Absender signierten Form vor.

Die Signatur des Ausgangsdokumentes dient der Nachweisbarkeit seiner Originalität. Um diese zu erhalten ist es notwendig, das Dokument in der signierten Form aufzubewahren.

Ein möglicher Angriffspunkt auf die Daten ist der private Schlüssel des Servers. Da alle eingelagerten Daten - genauer gesagt alle Session-Keys der eingelagerten Daten - mit demselben Schlüssel des Servers lesbar sind, lohnt sich ein Angriff auf diesen Schlüssel einerseits besonders, andererseits wird er durch die Menge vorliegender Daten erleichtert.

Um diesem Umstand vorzubeugen, wird bei einer bevorzugten Ausführungsform der vorliegenden Erfindung als zusätzlicher Sicherheitsmechanismus eine Zweiteilung des Session-Keys eingeführt.

Wie weiter oben beschrieben, werden die Ursprungsdaten mit einem N-stelligen (N vorzugsweise größer oder gleich 128) symmetrischen Schlüssel verschlüsselt. Dieser Schlüssel wird üblicherweise für die Übertragung asymmetrisch und nur für den Empfänger lesbar verschlüsselt. Die - auch gewaltsame - Entschlüsselung des Session-Keys reicht damit aus, um die Daten selbst entschlüsseln zu können.

Um dies zu verhindern, wird folgende Modifikation eingeführt. Bei dieser Modifikation wird der Session-Key vor seiner asymmetrischen Verschlüsselung zweigeteilt. Beispielsweise werden M ($0 < M < N$) der N Bits des Session-Keys als sogenannter "Vorgangsschlüssel" herausgelöst. Nur die verbleibenden (N-M) Bits des Session-Keys werden asymmetrisch verschlüsselt und mit den Daten übertragen.

Die Umschlüsselung der Daten mit reduziertem Session-Key kann in genau derselben Weise erfolgen, wie oben in Zusammenhang mit einem vollständigen Session-Key beschrieben. Da die Daten selbst auch dort nie entschlüsselt werden müssen, ist der vollständige Session-Key nicht notwendig. Es wird lediglich der rudimentäre Session-Key durch den Server entschlüsselt und für den Anforderer wieder verschlüsselt.

Die Entschlüsselung beim Empfänger unterscheidet sich von der oben beschriebenen Vorgehensweise dahingehend, daß nach der Entschlüsselung des Session-Keys mittels privatem Schlüssel des Empfängers dieser Session-Key um die beim Absender separierten M Bits des Vorgangsschlüssels erweitert werden muß. Danach kann die Entschlüsselung wie oben dargestellt erfolgen.

Der beim Absender der Daten erzeugte Vorgangsschlüssel, d.h. die separierten M Bits, wird an die ebenfalls dort erzeugte Vorgangs-ID angefügt. Die Kombination von Vorgangs-ID und Vorgangsschlüssel ergibt die sogenannte Vorgangskennung, die auf dem den Vorgang begleitenden Papierdokument (Überweisungschein, Einweisungsschein, Rezept, ...) aufgedruckt und beim Empfänger erfaßt wird. Der in der Vorgangskennung enthaltene Vorgangsschlüssel wird niemals zum Server übertragen, so daß dort nie alle Informationen zusammenkommen, die ausreichen würden, um ein Dokument tatsächlich zu entschlüsseln.

Ein Beispiel für eine erfindungsgemäße Vorrichtung, wie sie für die Durchführung des obigen Anwendungsbeispiels eingesetzt wird, ist in Figur 1 dargestellt.

Die Vorrichtung ist vorzugsweise in Form eines Einsteckmoduls 1 (Umschlüsselungsmodul) zum modularen Einbau in den Server ausgebildet. Das Modul 1 beinhaltet im vorliegenden Beispiel eine Chipkarte 2, die die Entschlüsselung des verschlüsselten Session-Keys 10a mit Hilfe des in der Chipkarte 2 gespeicherten privaten Schlüssels des Servers und die erneute Verschlüsselung des Session-Keys mit dem öffentlichen Schlüssel des Adressaten bzw. Anfordernden der Daten vornimmt. Der private Schlüssel des Servers ist dabei von außerhalb der Chipkarte bzw. des Moduls nicht zugänglich. Der öffentliche Schlüssel des Anfordernden wird der Vorrichtung 1, ebenso wie der umzuschlüsselnde Session-Key 10a über eine dafür vorgesehene Schnitt-

stelle zugeführt. Über eine weitere Schnittstelle wird der neu verschlüsselte Session-Key 10b ausgegeben.

Der Prozessor des Servers selbst übernimmt hierbei die Aufgabe, den Session-Key 10a von dem verschlüsselten Datenblock 11 abzutrennen, der Vorrichtung 1 zuzuführen und den von der Vorrichtung gelieferten, neu verschlüsselten bzw. umgeschlüsselten Session-Key 10b wieder an den Datenblock 11 anzufügen, wie in der Figur schematisch dargestellt ist.

Es ist allerdings auch möglich, diese Trennung und erneute Zusammenführung direkt in der Vorrichtung 1 vorzunehmen. Hierbei müßte der Vorrichtung der gesamte Datenblock 11 mit dem Session-Key 10a zugeführt werden.

Der persönliche Schlüssel des Servers ist zweifelsohne ein problematischer Punkt im Hinblick auf gezielte unberechtigte Zugriffsversuche auf die Daten.

Üblicherweise dürfen bzw. sollten Schlüssel nicht auf dem Rechner gespeichert werden, auf dem die verschlüsselten Daten gespeichert bzw. bearbeitet werden. Dies ist jedoch bei automatischer Arbeit des Servers, wie im vorliegenden Fall, unumgänglich. Aus diesem Grunde ist im vorliegenden Ausführungsbeispiel vorgesehen, die Vorrichtung als gekapselte und plombierte Einheit auszugestalten, die in der Lage ist, die vollständige Prozedur der Datenumschlüsselung intern zu handhaben, ohne daß der entschlüsselte (auch rudimentäre) Session-Key oder auch nur Spuren seiner Entschlüsselung die autonome Einheit verlassen.

Heutzutage sind bereits Schlüsselkarten am Markt verfügbar, die in der Lage sind, die asymmetrische Verschlüsselung eines 128 Bit Session-Keys nach einem

1024 Bit RSA-Verfahren vollständig auf dem Chip der Karte auszuführen. Demnächst werden solche Karten auch für 2048 Bit Schlüssel zur Verfügung stehen. Insbesondere besteht die Möglichkeit, das Schlüsselpaar (öffentlicher Schlüssel - privater Schlüssel) direkt auf der Karte oder in einem gesetzeskonformen, zertifizierten Trust-Center generieren zu lassen, ohne daß der private Schlüssel der Karte diese jemals verläßt. Eine solche Schlüsselkarte kann in der erfindungsgemäßen Vorrichtung als Chipkarte 2 eingesetzt werden. Hierbei wird dieser Karte 2 in einem ersten Schritt zunächst der verschlüsselte Session-Key 10a zugeführt. Dieser wird mit Hilfe des privaten Schlüssels des Karte, weiter oben als der private Schlüssel des Servers bezeichnet, entschlüsselt. Der entschlüsselte Session-Key wird von der Karte 2 ausgegeben, ohne die Vorrichtung 1 jedoch zu verlassen. Er wird vielmehr in einem zweiten Schritt der Karte 2 erneut, diesmal zusammen mit dem öffentlichen Schlüssel des Adressaten eingegeben. Die Karte 2 liefert in diesem zweiten Schritt den neu verschlüsselten Session-Key 10b zurück. Dies ist schematisch durch die Pfeile innerhalb der Vorrichtung 1 in der Figur angedeutet. Die hierfür zusätzlich erforderliche Schaltung, Puffer-Einheit 4, dient u.a. zur zeitlichen Koordination dieser Vorgänge. Diese Puffer-Einheit 4 kann beispielsweise durch einen geeignet programmierten Mikroprozessor oder mittels einer Logikschaltung realisiert werden.

Um zu verhindern, daß aus Modulationen auf der Stromversorgung der Vorrichtung Rückschlüsse auf die internen Abläufe möglich sind, ist in der vorliegenden Ausführungsform der Vorrichtung eine Konstant-

stromschaltung 3 vorgesehen, die garantiert, daß die Vorrichtung im Rahmen eines definierten Intervalls der Versorgungsspannung eine konstante und modulationsfreie Stromaufnahme vorweist. Bei Unter- oder Überschreiten bestimmter Grenzen der Betriebsspannung oder anderer Betriebsparameter, wie z.B. der Temperatur, schaltet sich die Vorrichtung mit einer Fehlermitteilung ab.

Da auch aus dem Zeitverhalten der Vorrichtung Rückschlüsse auf die internen Vorgänge gezogen werden könnten, können alle Eingangsdaten zunächst in der Puffer-Einheit 4 oder einer speziell dafür vorgesehenen Einheit gepuffert, und nach einer ständig gleichen Zeit die Ergebnisse ausgegeben werden, unabhängig davon, weiche Zeit die internen Abläufe in Anspruch genommen haben.

Ein "Abhören" der elektromagnetischen Vorgänge in der Vorrichtung wird im vorliegenden Ausführungsbeispiel durch eine elektromagnetische Abschirmung 5 der Vorrichtung verhindert.

Als Schnittstelle der Vorrichtung ist einerseits eine Schnittstelle für die Eingabe des asymmetrisch verschlüsselten Session-Keys 10a (bzw. des Rudimentes dieses Schlüssels) und des öffentlichen Schlüssels des anfordernden Empfängers vorgesehen. Andererseits muß eine Schnittstelle für die Ausgabe des asymmetrisch verschlüsselten Session-Keys 10b (bzw. dessen Rudiment) vorhanden sein. Beide Schnittstellen können bei geeigneter Ausführung physikalisch identisch sein.

Weiterhin können für die Erzeugung bzw. Überprüfung von Signaturen Schnittstellen für die

Eingabe des Hash-Wertes des zu signierenden Dokumentes und für die Ausgabe des symmetrisch verschlüsselten Hash-Wertes, d.h. der Signatur vorgesehen sein.

Obwohl die vorangehend beschriebenen Maßnahmen in Zusammenhang mit dem zugrunde liegenden Beispielfall dargestellt wurden, lassen sich dieses Konzept und die erfindungsgemäße Vorrichtung selbstverständlich auch auf andere Bereiche anwenden, bei denen eine sichere Datenübertragung zwischen zwei Datenstationen über eine Zwischenlagerung auf einem Server erforderlich ist.

Weiterhin ist die Erfindung nicht auf die Weiterleitung der Daten nur über eine Zwischenstation bzw. einen Server beschränkt. So können die Daten auch über mehrere Server geleitet werden, wobei der Abruf der Daten durch einen weiteren Server jeweils wie der Abruf durch einen Adressaten ausgeführt wird. Auf dem weiteren Server werden dann die Daten in gleicher Form wie auf dem ersten Server behandelt, d.h. auch dieser weitere Server muß die erfindungsgemäße Vorrichtung aufweisen.

Patentansprüche

1. Vorrichtung für die sichere Übertragung bzw. Weiterleitung von verschlüsselten Daten über eine Datenstation eines Netzwerkes, mit
- einer Eingangseinheit zum Empfangen der verschlüsselten Daten (10a) sowie eines externen Schlüssels,
- einer Einheit (2) zum Entschlüsseln der verschlüsselten Daten mit einem internen Schlüssel und zum erneuten Verschlüsseln der Daten mit dem externen Schlüssel, wobei der interne Schlüssel von außerhalb der Vorrichtung nicht zugänglich ist; und
- einer Ausgangseinheit zum Ausgeben der mit dem externen Schlüssel verschlüsselten Daten (10b).

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß der interne Schlüssel innerhalb der Einheit (2) zum Entschlüsseln und Verschlüsseln auf einem geeigneten Datenträger gespeichert ist.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln eine Chipkarte als Träger des internen Schlüssels umfaßt.

4. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln eine aktive Chipkarte mit integriertem Prozessor umfaßt, die die Ent- und Verschlüsselung der Daten ganz oder teilweise übernimmt.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß sie eine Puffer- und Logik-Einheit (4) zur zeitlichen Steuerung des Datenflusses in der Vorrichtung aufweist, die der Einheit (2) zum Entschlüsseln und Verschlüsseln zunächst die verschlüsselten Daten (10a) zur Entschlüsselung zuführt und entschlüsselt zurückerhält, und die anschließend der Einheit (2) zum Entschlüsseln und Verschlüsseln die entschlüsselten Daten zur Verschlüsselung mit dem externen Schlüssel zuführt und als verschlüsselte Daten (10b) zurückerhält.

6. Vorrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Eingangseinheit und die Ausgangseinheit Standardschnittstellen für die Ein- und Ausgabe der Daten aufweisen.

7. Vorrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln asymmetrische Verschlüsselungsverfahren einsetzt.

8. Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß sie mit einer vollständigen mechanischen und elektromagnetischen Kapselung (5) und mit einer Möglichkeit zur Versiegelung versehen ist.

9. Vorrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß eine Puffer-Einheit vorgesehen ist, die alle Datenströme innerhalb der Vorrichtung zum Ausgleich von eventuell vom internen Schlüssel abhängigen Verarbeitungszeiten puffert, so

daß die Ausgabe der Daten der Vorrichtung nach einer prozeßunabhängigen Zeitspanne erfolgt.

10. Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß eine Einheit (3) zum Puffern der Stromaufnahme der Vorrichtung vorgesehen ist, so daß die Stromaufnahme der Vorrichtung unabhängig von der vom internen Schlüssel abhängigen Stromaufnahme der Einheit (2) zum Entschlüsseln und Verschlüsseln oder weiterer interner Schaltkreise ist.

11. Vorrichtung nach einem der Ansprüche 1 bis 10, die weiterhin eine Einheit zum Empfangen eines ersten Datenblockes, der die verschlüsselten Daten (10a) neben weiteren Daten (11) beinhaltet, und zum Abtrennen der verschlüsselten Daten (10a) von den weiteren Daten (11) sowie eine Einheit zum Zusammenführen der weiteren Daten (11) mit den erneut verschlüsselten Daten (10b) zu einem zweiten Datenblock und zur Ausgabe des zweiten Datenblockes aufweist, wobei die verschlüsselten Daten einen Schlüssel darstellen, mit dem die weiteren Daten (11) verschlüsselt sind.

12. Verfahren für die sichere Übertragung von Daten von einer ersten Datenstation über eine zweite Datenstation zu einer dritten Datenstation unter Einsatz der Vorrichtung gemäß einem der vorangehenden Ansprüche, mit folgenden Schritten:

- Verschlüsseln der Daten in der ersten Datenstation mit einem ersten Schlüssel;
- Verschlüsseln zumindest eines Teils des ersten Schlüssels in der ersten Datenstation mit einem öffentlichen Schlüssel der zweiten Datenstation;

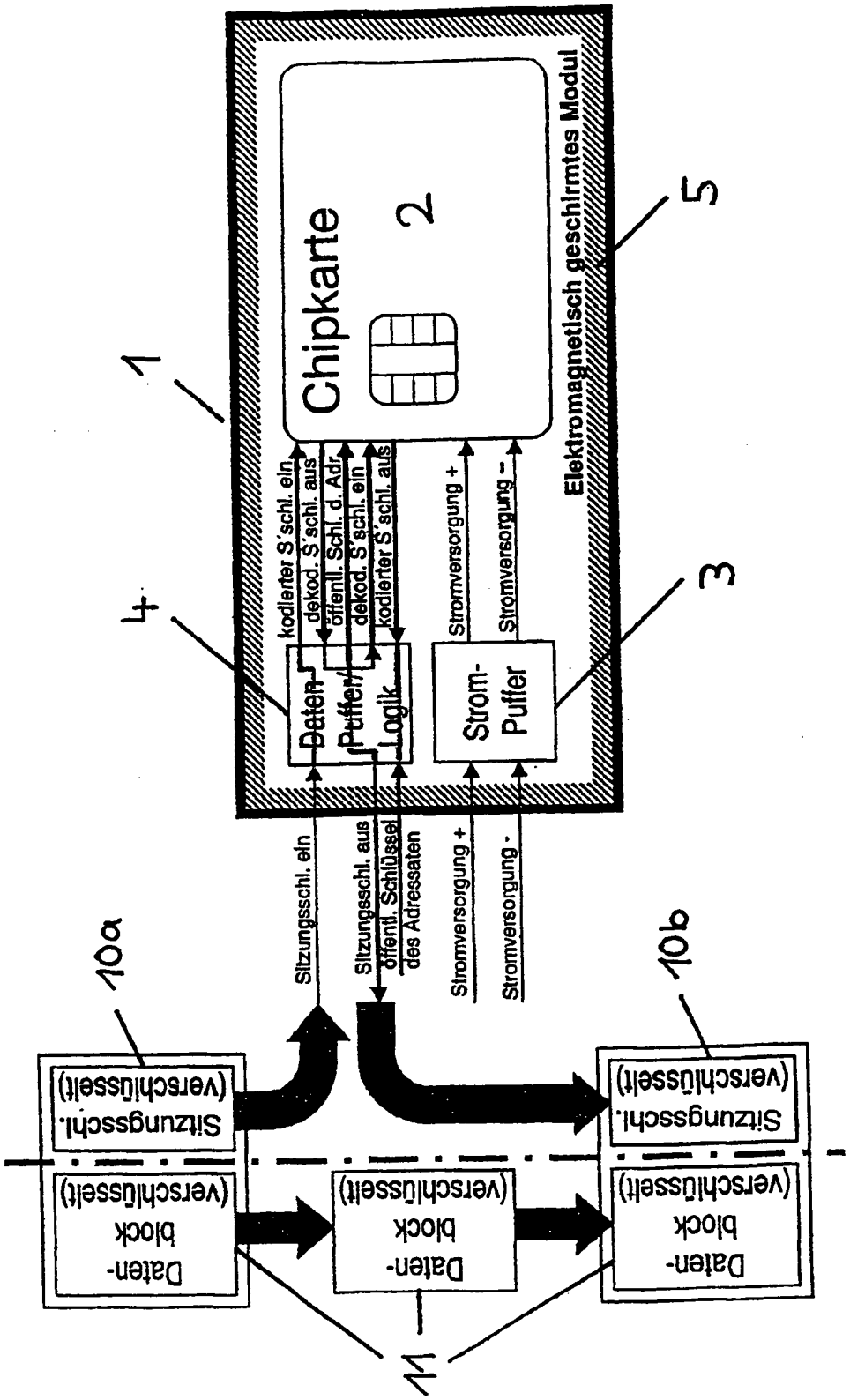
- Übermitteln der verschlüsselten Daten (11) zusammen mit dem verschlüsselten Teil des ersten Schlüssels (10a) an die zweite Datenstation;
- Speichern der verschlüsselten Daten (11) und des verschlüsselten Teils des ersten Schlüssels (10a) in der zweiten Datenstation;
- Anfordern der Daten durch die dritte Datenstation;
- Entschlüsseln des verschlüsselten Teils des ersten Schlüssels in der zweiten Datenstation mit einem zum öffentlichen Schlüssel passenden privaten Schlüssel der zweiten Datenstation und erneutes Verschlüsseln des vorher entschlüsselten Teils des ersten Schlüssels mit einem öffentlichen Schlüssel der dritten Datenstation; und
- Übermitteln der verschlüsselten Daten (11) zusammen mit dem erneut verschlüsselten Teil des ersten Schlüssels (10b) an die dritte Datenstation.

13. Verfahren nach Anspruch 12, wobei der erste Schlüssel vollständig verschlüsselt und übermittelt wird.

14. Verfahren nach Anspruch 12, wobei nur ein Teil des ersten Schlüssels verschlüsselt und an die zweite Datenstation übermittelt wird.

15. Verfahren nach einem der Ansprüche 12 bis 14, wobei der verschlüsselte Teil des ersten Schlüssels in der dritten Datenstation mit dem privaten Schlüssel der dritten Datenstation entschlüsselt wird, und anschließend die Daten (11) mit dem ersten Schlüssel entschlüsselt werden.

16. Verfahren nach einem der Ansprüche 12 bis 15, wobei der öffentliche Schlüssel der dritten Datenstation aus einer internen Datenbank der zweiten Datenstation entnommen oder durch Rückfrage bei einem Trust-Center ermittelt wird.



BERICHTIGTES BLATT (REGEL 91)

5551

CERTIFICATION

I, the undersigned, am a professional translator, fully competent to translate from German into English, and I declare hereby that the attached English rendition of the PCT International Preliminary Examination Report dated May 31, 2001 as issued in International Application PCT/DE00/00189 filed January 20, 2000 is a genuine translation, accurate in every particular, to the best of my ability and knowledge.

Name: Michaela Nierhaus
Address: Brabanterstr. 15
80805 Munich
Germany

Date: Oct. 4, 2001

International Preliminary Examining Report of 31/05/01

---

1. This internal preliminary examining report is issued by the Office assigned therewith and is forwarded to the applicant in accordance with Article 36.

2. This report comprises all told 8 pages including the cover page.

   Moreover. The report is accompanied by ENCLOSURES; these are pages with specification, claims and/or drawings which have been altered and are the basis of this report, and/or pages with amendments made before this authority (see Rule 70.16 and Section 607 of the Guidelines for PCT)

   These enclosures comprise all told 3 pages.

I	X	Basis of the report
V	X	Reasoned opinion according to Rule 35(2)regarding novelty, inventive step and commercial applicability: documents and explanation in support thereof
VII	X	Specific shortcomings of the international application
VIII	X	Specific remarks concerning the international application

I. Basis of the Report

1.This report was drawn up on the basis (replacement pages filed upon request by the Office according to Article 14 shall be considered within the scope of this report as "originally filed".)

Specification, Pages:
1-20 original version

Claims, Nos.:
2-11,13-16 original version

1,12 submitted on 25/04/2001 with letter of 24/04/2001

Drawings, pages:
1/1 original version

V. Reasoned opinion to according Rule 66.2a)ii) regarding novelty, inventive step and commercial applicability: documents and explanation in support thereof

1. Opinion

Novelty (N)	Yes: Claims 1-16
Inventive step (IS)	Yes: Claims 1-16
Commercial applicability (CA)	Yes: Claims 1-16

2. Documents and Explanations
see accompanying page

VII. Specific shortcomings of the international application
It was determined that the international application shows the following shortcomings as to form and content:
see accompanying page

VIII. Specific remarks concerning the international application
For clarity of the claims, of the specification and the drawings or whether or not the claims are fully supported by the specification, the following is to be noted:
see accompanying page

INTERNATIONAL PRELIMINARY REPORT
ACCOMPANYING PAGE

To SECTION V:

1). According to its title, the international application PCT/DE00/189 is concerned with a device and a method for secure electronic data processing. Claim 1 describes a device and the independent claim 12 the process.

2). The **nearest state of the art** according to the international search report are documents **D1** and **D2.**

D1: EP-A-0 869 652 (TUMBLEWEED SOFTWARE CORP) 7 October 1998 (1998-10-07)
D2: US-A-5 751 813 (DORENBOS DAVID) 12 MAY 1998 (1998-05-12)

The generic part of claim 1 is based on the disclosure of D2.

The drawback of the state of the art are explained on page 2, second and third paragraph as well as on page 6, lines 15 to 31.

- The **object of the invention** is (cf. Page 2, last paragraph) to provide a device and a method for secure data transmission via the server of a network wherein the addressee of the data does not need to be known at the time the data is available.

4a). The object of the present invention is solved by the advantageous interaction of the technical features set forth in claim 1. The device of claim 1 is shown in figure 1.
Claim 1 states:
A device for secure transmission respectively forwarding of coded data
from a first data station
via a second data station
to a third data station of a network,
having
- an input unit
for receiving said coded data (10a) from said first data station
and
for receiving a requester's external key from said third or a further data station,
- a unit (2)
for recoding said coded data by means of decoding with an internal key and recoding with said external key, with said internal key not being accessible from outside said device:
and
- an output unit for issuing said data (10b) encoded with said external key,

wherein
said device is designed *in such a manner* on or in said second data station
that said unit (2) recodes the data only after request by said third data station with the aid of said requester's external key and
the data do not leave said device during recoding,
so that the data are not accessible in uncoded form on said second data station from outside said device.

4b). The objet of the present invention is solved by the advantageous interaction of the technical features set forth in independent claim 12.
Claim 12 states:
A method for secure transmission of data
from a first data station
via a second data station
to a third data station
using the *device according to one of the preceding claims* on
or in said second data station,
having the following steps:

- encoding the data **in said first data station** with a first key (10a),
- dividing said first key (10a) into a first part and a second part in such a manner that neither said first nor said second part alone permit decoding the coded data;
- encoding said first part of said first key (10a) in said first data station with the public key of said second data station;

- transmission of said coded data (11) together with said coded first part of said first key (10a) to said second data station;
- storage of said coded data (11) and of said coded first part of said first key (10a) **in said second data station;**
- request of said data by said third data station, the identity of which is unknown to said second data station until it is informed by the request;
- decoding of said coded first part of said first key in said second data station with a private key of said second data station matching said public key
  and
  recoding of said previously decoded first part of said first key with a public key of said third data station; and
- transmission of said coded data (11) together with said recoded first part of said first key (10b) to said third data station;

- decoding of said coded first part of said first key (10b) **in said third station** with a private key matching the public key of said third station;
- completion of said first key (10a) in said third station by adding said first part to said second part of said first key which was transmitted on a separate path from said first data station to said third data station;
- decoding said coded data (11) with the complete first key (10a) in said third data station.

5. The subject matter described in claims 1 and 12 develop advantageous effects as explained on page 7 (last paragraph) of the specification.

6. **None** of the documents of the international search report alone discloses all the technical features of claim 1 respectively of independent claim 12. The subject matter of claims 1 respectively 12 , therefore, fulfill the criterium of novelty (Art.33(10 and (2)PCT). The subject matter of claim 1 respectively 12 are also **not** obvious from the documents cited in the international search report. Therefore the requirements regarding inventive step of the claims subject matter are fulfilled (Article 33(1) and (3)PCT).
Commercial applicable is the subject matter of claims 1 respectively 13, i.a. in the field of

transmitting medical data. Consequently, the requirements of Article 33(1) and (4) PCT are fulfilled.

7. The dependent claims 2 to 11 and 13 to 16 define special designs of the device according to claim 1 respectively of the process according to claim 12, which principally and subject to the remarks in section VIII also fulfill the requirements with regard to novelty, inventive step and commercial applicability (Art. 33(2) to (4)PCT).

To Section VII:

1). Documents **D1** and **D2** were not cited in the specification; nor was the **state of the art** contained therein briefly described. The requirements of Rule 5.1(a)(ii)PCT are therefore not fulfilled.

2). The specification (cf. page 3, second paragraph ff.) was not adapted to the pertinent claims. Thus the requirements of Rule 5.1(a)(iii)PCT are not fulfilled.

3). Figure1/1 uses some expressions such as "receivers p'key" etc. which are not part of the language of the proceedings (German) and therefore do not fall in the category of known technical terms. These terms have to be replaced by understandable terms of the language of the proceedings. The English terms may continued to be used if set in brackets.

The applicant has said he will make respective amendments or adaptations upon entering in the regional or patenting phase.

To Section VIII:

The original, dependent claims 2 to 11 and 13 to 16 were not adapted to the amended independent claims 1 and 12. Thus there partly are objections regarding Article 6 PCT, because the additional features of the independent claims cause ambiguity (e.g. claim 13) or because the additional features of the independent claims have meanwhile become superfluous (e.g. claims 14 and 15) and the claims are therefore no longer concise.

The applicant has said he will make respective amendments or adaptations upon entering in the regional or patenting phase.

New Claims 1 and 12

1. A device for secure transmission respectively forwarding of coded data from a first data station via a second data station to a third data station of a network, having

- an input unit for receiving said coded data (10a) from said first data station and for receiving a requester's external key from said third or a further data station;
- a unit (2) for recoding said coded data by means of decoding with an internal key and renewed encoding with said external key, with said internal key not being accessible from outside said device; and
- an output unit for issuing said data (10b) encoded with said external key;

wherein said device is designed in such a manner on or in said second data station that said unit (2) recodes said data only upon request by said third data station with the aid of said requester's external key and said data do not leave said device during recoding, so that said data are not accessible in uncoded form on said second data station from outside said device.

12. A method for secure transmission of data from a first data station via a second data station to a third data station using the device according to one of the preceding claims on or in said second data station, having the following steps:

- encoding the data in said first data station with a first key (10a);
- dividing said first key (10a) into a first part and a second part in such a manner that neither said first nor said second part alone permit decoding the coded data;
- encoding said first part of said first key (10a) in said first data station with the public key of said second data station;
- transmission of said coded data (11) along with said coded first part of said first key (10a) to said second data station;

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts 990202PCT	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/DE 00/ 00189	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 20/01/2000	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)* 29/03/1999
Anmelder FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG.et al		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [ ] wie vom Anmelder vorgeschlagen

   [ ] keine der Abb.

   [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 00/00189

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/30 H04L9/08 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 869 652 A (TUMBLEWEED SOFTWARE CORP) 7. Oktober 1998 (1998-10-07) Seite 14, Zeile 42 -Seite 17, Zeile 30; Abbildung 3	1,2,6,7, 11-13, 15,16
Y		3,4,8

X	US 5 751 813 A (DORENBOS DAVID) 12. Mai 1998 (1998-05-12) Spalte 2, Zeile 5 - Zeile 67	1

	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
6. Juni 2000	28/06/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Carnerero Álvaro, F

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

[redacted]tionales Aktenzeichen
PCT/DE 00/00189

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0869652	A	07-10-1998	US	6061448 A	09-05-2000
			JP	11031127 A	02-02-1999
US 5751813	A	12-05-1998	AU	3877997 A	19-11-1997
			BR	9702187 A	29-06-1999
			CA	2224661 A	06-11-1997
			EP	0882340 A	09-12-1998
			JP	11509075 T	03-08-1999
			PL	324266 A	11-05-1998
			WO	9741661 A	06-11-1997

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	ISHII S ET AL: "A HIGH-SPEED PUBLIC KEY ENCRYPTION PROCESSOR" SYSTEMS & COMPUTERS IN JAPAN,US,SCRIPTA TECHNICA JOURNALS. NEW YORK, Bd. 29, Nr. 1, 1. Januar 1998 (1998-01-01), Seiten 20-31, XP000742968 ISSN: 0882-1666 Seite 20 Seite 26	3,4,8
A	---	5,9,10
A	MENEZES, VAN OORSCHOT, VANSTONE: "Handbook of Applied Cryptography" , CRC PRESS , BOCA RATON, FLORIDA, USA; XP002139553ISBN: 0-8493-8523-7 Seite 524 -Seite 525	14

US 0993781905P1

Creation date: 10-25-2004
Indexing Officer: HNGUYEN13 - HIEU NGUYEN
Team: OIPEBackFileIndexing
Dossier: 09937819

Legal Date: 11-05-2001

No.	Doccode	Number of pages
1	M905	2

Total number of pages: 2

Remarks:

Order of re-scan issued on .....